UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/792,236	03/03/2004	Michael Thomas Kurdziel	RF-234 (50588)	4669

74701 7590 06/20/2008

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
06/20/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/792,236	KURDZIEL, MICHAEL THOMAS	
	Examiner	Art Unit	
	Christian LaForgia	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/3/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-38 have been presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 03 March 2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement has been considered by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,108,421 to Kurdziel et al., hereinafter Kurdziel, in view of U.S. Patent Application Publication No. 2004/0131182 A1 to Rogaway, hereinafter Rogaway.

5. As per claims 1 and 13, Kurdziel teaches a block cipher device and a communication system for a cryptographically secured digital communication system comprising:

a pair of first stages connected in parallel (Figure 4 [element 10], column 2, lines 10-13, i.e. serially or in parallel) and receiving an input data block and a control data block (claim 1(a) a first stage to receive an input data block and control data block), each first stage defining a respective first data path and comprising

a sum modulo-two unit responsive to the control data block and the input data block (claim 1(a)(i) a sum modulo-two unit responsive to the input data block and a first subset of the control data block), and

a first nibble swap unit downstream from said sum modulo-two unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said sum modulo-two unit (claim 1(a)(ii) a first nibble swap unit responsive to the output signal from said sum modulo-two unit and a second subset of the control data block for reordering the output signal from said sum modulo-two unit);

a key scheduler receiving a key data block and generating a random key data block based thereon (claim 1(b) a key scheduler responsive to a key data block including means for randomizing the key data block);

a pair of second stages connected in parallel (column 2, line 13, i.e. serial and parallel are interchangeable based on the intended use) downstream from said first stages and receiving the random key data block, the control data block and output signals from said first stages, each second stage defining a respective second data path (claim 1(c) a second stage adapted to receive the randomized key data block from said key scheduler in first and second key data sub-blocks, the control data block and the output signal from said first stage) and comprising

a first linear modulo unit responsive to the random key data block, one of the output signals from said first stages, and the control data block for performing a modulo summing operation based on a first modulus q (claim 1(c)(i) a first linear modulo unit responsive to said first key data sub-block from the key scheduler, the output signal from said first stage, and the control data block for performing a modulo summing operation based on a first modulo q),

an n^{th} power modulo unit responsive to an output signal from said first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p (claim 1 (c)(ii) an n^{th} power modulo unit responsive to the output signal from said first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p), and

a second linear modulo unit responsive to the random key data block and an output signal from said n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r (claim 1(c)(iii) a second linear modulo unit responsive to the second key data sub-block and output from said n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r),

each first, second and third modulus q, p and r being unique from each other (claim 1 said first, second, and third modulus p, q, and r respectively being unique from each other); and

an output stage connected to said second stages for generating an output data block for the block cipher device (Figure 4 [element 11], column 2, lines 9-14).

6. Kurdziel does not teach a diffuser connected in both of the first data paths for mixing data therebetween.

7. Rogaway discloses an intermediate step that mixes the bits (Abstract, paragraphs 0045, 0054, 104) in a parallel block cipher (paragraphs 0047, 0090).

8. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a diffuser connected in both of the first data paths for mixing data therebetween, since Rogaway states at paragraph 0081 that mixing the intermediate value preserves its length, thereby making encryption more secure by having data and a key of a predetermined length.

9. Regarding claims 2 and 18, Kurdziel teaches wherein said first and second stages are selectively configurable so that one first data path and one second data path are operational (Figure 4, column 2, line 10-15).

10. As noted above, Kurdziel does not disclose a diffuser, nor that it would be bypassed.

11. It would have been obvious to one of ordinary skill in the art at the time the invention was made since it has been held that it only requires routine skill in the art to eliminate an element and its function. See MPEP 2144.04; see *Ex parte Wu*, 10 USPQ 2031 (Bd. Pat. App. & Inter. 1989). This is further supported by the fact that Kurdziel discloses a similar system that functions without the diffuser mixing bits.

12. Regarding claims 3 and 19, Rogaway teaches wherein said diffuser is connected in both of the first data paths between the respective sum modulo-two units and first nibble swap units (paragraphs 0045, 0054, 104).

13. Regarding claims 4 and 20, Kurdziel teaches wherein each first stage further comprises a substitution/expansion unit downstream from said first nibble swap unit and being responsive to an output signal therefrom for providing customizable cipher variations (claim 2).

14. With regards to claims 5 and 21, Kurdziel teaches a second nibble swap unit downstream from said substitution/expansion unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said substitution/expansion unit (claim

3).

15. Regarding claims 6 and 22, Kurdziel teaches a nibble interleave unit connected in both of the first data paths for reordering data therebetween (Figure 4 [element 4], column 3, lines 5-17, i.e. re-ordering of W_3).

16. Regarding claims 7 and 23, Kurdziel teaches a substitution unit connected in both of the first data paths for substituting data therebetween (Figure 4 [element 3], column 2, line 62 to column 3, line 4).

17. Regarding claims 8 and 24, Kurdziel teaches wherein each n^{th} power modulo unit provides an output signal of predetermined size, with $n>1$ and with $p=2^K-X$, where X is selected such that a greatest common denominator between n and (2^K-X-1) is 1 and K is the predetermined size (claim 1(c)(ii)).

18. Regarding claims 9 and 25, Kurdziel teaches wherein said key scheduler comprises a pair of look-up tables for generating the random key data block (claim 5).

19. With regards to claims 10 and 26, Kurdziel teaches wherein said key scheduler further comprises a pair of shift registers responsive to the received key data block (claim 6); and wherein each look-up table is responsive to a corresponding shift register (claim 7).

20. Concerning claims 11 and 27, Kurdziel teaches wherein said key scheduler further comprises a pair of combiners responsive to outputs from said shift registers and to outputs from said look-up tables, each combiner combining the output from a corresponding shift register and the output from a corresponding look-up table using a modulo-two summing operation, and each combiner providing a combined data output (claim 8).

21. Regarding claims 12 and 28, Kurdziel teaches wherein each second stage further comprises a non-invertible operation unit downstream from said n^{th} power modulo unit and being responsive to an output signal therefrom, said non-invertible operation unit discarding a portion of the output signal from said n^{th} power modulo unit (claim 13).

22. Regarding claim 14, Kurdziel teaches wherein said first unit comprises a sum modulo-two unit, said second unit comprises a nibble swap unit, and said first and second modulo units comprise first and second linear modulo units for performing summing operations (claim 11).

23. Regarding claim 15, Kurdziel teaches wherein said block cipher device operates as an encrypter (column 1, lines 30-33).

24. Regarding claim 16, Kurdziel teaches wherein said block cipher device operates as a decrypter (column 1, lines 30-33).

25. Regarding claim 17, Kurdziel teaches further comprising circuitry connected to said

block cipher device so that said block cipher device operates in at least one of a block cipher feedback mode, a minimum error propagation mode and a self-synchronizing feedback mode (column 4, lines 38-41).

26. As per claim 29, Kurdziel teaches a method for converting an input data block into an output data block for a cryptographically secured digital communication system, the method comprising:

providing the input data block, a control data block and a random key data block to parallel data paths (column 2, line 13, i.e. serial or in parallel) in the digital communication system (claim 15(a) providing an initial data block, a control data block, a first key data block and a second key data block);

combining the control data block and the input data block within each data path to provide a first data output signal for each data path (claim 15(b) combining the initial data block and the control data block to provide a first data output signal);

transposing segments of the first data output signal within each data path in response to the control data block to provide a second data output signal within each data path (claim 15(c) transposing segments of the first data output signal responsively to a first subset of the control data block to provide a second data output signal);

performing a first linear modulo operation based on a modulus q within each data path in response to the second data output signal, the random key data block and the control data block to provide a third data output signal within each data path (claim 1(c)(i) a first linear modulo unit responsive to said first key data sub-block from the key scheduler, the output signal from said

first stage, and the control data block for performing a modulo summing operation based on a first modulo q);

performing an n^{th} power modulo operation based on a second modulus p within each respective data path in response to the third data output signal to provide a fourth data output signal within each data path (claims 1 (c)(ii), 15(g) an n^{th} power modulo unit responsive to the output signal from said first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p); and

performing a second linear modulo operation based on a third modulus r within each respective data path in response to the random key data block (claim 1(c)(iii) a second linear modulo unit responsive to the second key data sub-block and output from said n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r) and the fourth data output signal to provide an output data block (Figure 4 [element 11], column 2, lines 9-14),

each first, second and third modulus q, p and r being unique from each other (claim 1 said first, second, and third modulus p, q, and r respectively being unique from each other).

27. Kurdziel does not teach mixing data between the parallel data paths.

28. Rogaway discloses an intermediate step that mixes the bits (Abstract, paragraphs 0045, 0054, 104) in a parallel block cipher (paragraphs 0047, 0090).

29. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a diffuser connected in both of the first data paths for mixing data therebetween, since Rogaway states at paragraph 0081 that mixing the intermediate value preserves its length, thereby making encryption more secure by having data and a key of a predetermined length.

30. Regarding claim 30, Kurdziel teaches wherein the cryptographically secured digital communication system is selectively configurable so that one data path is operational (Figure 4, column 2, line 10-15).

31. Regarding claim 31, Kurdziel teaches performing a substitution/expansion operation within each data path on the second data output signal to provide customizable cipher variations (claim 2).

32. With regards to claim 32, Kurdziel teaches performing a nibble swap operation within each data path on the customizable cipher variations in response to the control data block for reordering the customizable cipher variations (claim 3).

33. Concerning claim 33, Kurdziel teaches performing a nibble interleave operation for reordering data between the data paths for the reordered customizable cipher variations (Figure 4 [element 4], column 3, lines 5-17, i.e. re-ordering of W_3).

34. Concerning claim 34, Kurdziel teaches performing a substitution operation after the nibble interleave operation for substituting the reordered customizable cipher variations between the parallel data paths (Figure 4 [element 3], column 2, line 62 to column 3, line 4).

35. Regarding claim 35, Kurdziel teaches wherein each n^{th} power modulo unit provides an

output signal of predetermined size, with n>1 and with $p=2^K-X$, where X is selected such that a greatest common denominator between n and (2^K-X-1) is 1 and K is the predetermined size (claim 1(c)(ii)).

36. Regarding claim 36, Kurdziel teaches wherein the random key data block is generated by a key scheduler comprising a pair of look-up tables (claim 5).

37. With regards to claim 37, Kurdziel teaches wherein the key scheduler further comprises a respective shift register associated with each look-up table (claims 6 and 7).

38. Concerning claim 38, Kurdziel teaches wherein the key scheduler further comprises a pair of combiners responsive to outputs from the shift registers and to outputs from the look-up tables, each combiner combining the output from a corresponding shift register and the output from a corresponding look-up table using a modulo-two summing operation, and each combiner providing a combined data output (claim 8).

Double Patenting

39. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined

application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

40. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

41. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

42. Claims 1-38 are rejected on the ground of nonstatutory double patenting over claims 1-27 of U. S. Patent No. 6,108,421 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

43. The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: It appears that the instant application is claiming the parallel version of the earlier claimed invention implemented serially. The instant application differs from the claims of the patent in that the present application does the calculation in parallel, while the claims of the

patent perform it serially. Column 2, line 13 states that performing the function in serial or in parallel usually depends on the application. Furthermore, the claims of the instant application include "a diffuser connected in both of the fist data paths for mixing data therebetween." This element is not discussed in the previously filed application that has matured into a patent, although it would have been obvious to one of ordinary skill in the art to include it in the inventor's first application for the reasons discussed above.

44. Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See also MPEP § 804.

Conclusion

45. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

46. The following patents are cited to further show the state of the art with respect to parallel block ciphers with mixing functions, such as:

United States Patent No. 6,182,216 B1 to Luyster, which is cited to show a parallel block cipher with bit diffusion.

United States Patent No. 6,199,162 B1 to Luyster, which is cited to show a parallel block cipher with bit diffusion.

United States Patent No. 6,578,150 B2 to Luyster, which is cited to show a parallel block cipher with bit diffusion.

United States Patent No. 6,751,319 B2 to Luyster, which is cited to show a parallel block cipher with bit diffusion.

United States Patent No. 6,769,063 B1 to Kanda et al., which is cited to show a block cipher with a data diffusion part that randomizes input data.

United States Patent Application Publication No. 2001/038693 A1 to Luyster, which is cited to show a parallel block cipher with bit diffusion.

United States Patent Application Publication No. 2003/0174835 A1 to Yokota, which is cited to show a block cipher with a data diffusion unit.

47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

48. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

49. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf